Free Questions for XSIAM-Engineer

Shared by Bullock on 24-03-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A Cortex XSIAM engineer plans to add Kafka and Syslog Collectors to a Broker VM cluster.

What are two expected behaviors of the applets when they are added to the cluster? (Select two.)

Options:

A- Syslog Collector applet is automatically initiated, enters an active state on the primary node, and is on standby on the standby nodes.
B- Kafka Collector applet is automatically initiated, enters an active state on the primary node, and is on standby on the standby nodes.
C- Syslog Collector applet is active on all cluster nodes, including primary and standby.
D- Kafka Collector applet is active on all cluster nodes, including primary and standby.

Answer:

A, D

Explanation:

In a Broker VM cluster, the Syslog Collector applet runs in active/standby mode (active on the primary node, standby on others), while the Kafka Collector applet runs in active/active mode (active on all nodes). This design ensures both high availability and scalability for ingestion.

Question 2

Question Type: MultipleChoice

Which type of parsing error is categorized in the dataset "parsing_rules_errors"?

Options:

A- Compilation
B- Unrecognized code
C- Invalid syntax

D- Data mismatch

Answer:

A

Explanation:

The parsing_rules_errors dataset records compilation errors that occur when a parsing rule cannot be properly built or executed. This helps engineers identify and fix issues in rule definitions before logs are processed.

Question 3

Question Type: MultipleChoice

Which field is automatically mapped from the dataset to the data model when creating a data model rule?

Options:

A- _event_type
B- _insert_time
C- _host_name
D- _cloud_id

Answer:

A

Explanation:

When creating a data model rule, the field _event_type is automatically mapped from the dataset to the data model. This ensures events are categorized correctly in alignment with the Cortex XSIAM Data Model (XDM).

Question 4

Question Type: MultipleChoice

Using the integrationContext object, how is data stored and retrieved between integration command runs in Cortex XSIAM?

Options:

A- The integrationContex object can only store strings, not key-value dictionaries.
B- The integrationContex object is retrieved and set using the test-module command.
C- The get_integration_context() method overrides the existing object that is stored.
D- The integrationContex object supports get_integration_context() and set_integration_context().

Answer:

D

Explanation:

The integrationContext object in Cortex XSIAM is persistent across integration command runs and is managed using get_integration_context() and set_integration_context(). This allows data (such as key-value dictionaries) to be stored and retrieved reliably between executions.

Question 5

Question Type: MultipleChoice

An engineer needs to migrate Cortex XDR agents without internet connection from Cortex XSIAM tenant A to Cortex XSIAM tenant B. There is a broker configured for each tenant. This is the communication flow:

XDR agents <-> Broker A <-> XSIAM tenant A

XDR agents <-> Broker B <-> XSIAM tenant B

Which two steps should be taken before moving the agents? (Select two.)

Options:

A- Install a new Broker C on site B, and register it into Cortex XSIAM tenant A.
B- Install a new Broker C on site and register it into Cortex XSIAM tenant B.
C- Also register Broker A to Cortex XSIAM tenant B.
D- Select all endpoints in the console and add a new Broker C as proxy.

Answer:

B, C

Explanation:

To migrate XDR agents without internet from tenant A to tenant B, the engineer must install a new Broker C registered to tenant B to establish communication, and also register Broker A with tenant B so existing agents can transition their communication path smoothly during migration.

Question 6

Question Type: MultipleChoice

What is a key characteristic of a parsing rule in Cortex XSIAM?

Options:

A- It uses regular expressions exclusively for data modifications, discards unmatched logs by default, and only retains fields with non-null values.
B- It is bound to all vendors and products, performs data parsing once per log, and does not allow grouping.
C- It is bound to a specific vendor and product, performs data parsing once per log, and does not allow grouping.
D- It is bound to a specific vendor and product which allow grouping with a no-match policy, and retains all fields.

Answer:

C

Explanation:

A parsing rule in Cortex XSIAM is bound to a specific vendor and product, ensuring accurate parsing logic for that log source. It processes each log individually (once per log) and does not

allow grouping, making it distinct from data model rules.

Question 7

Question Type: MultipleChoice

A security engineer notices that in the past week ingestion has spiked significantly. Upon investigating the anomaly, it is determined that a custom application developed in-house caused the spike. The custom application is sending syslog to the Broker VM Syslog Collector applet. The engineer consults with the SOC analyst, who determines that 90% of the logs from the custom application are not used.

What can the engineer configure to reduce the ingestion?

Options:

A- Parsing rule to drop the unnecessary data at the Broker VM
B- Data model rule to drop the unnecessary data
C- Correlation rule on the Cortex XSIAM server to drop the unnecessary data
D- Data model rule to map the useful data

Answer:

A

Explanation:

To reduce ingestion from the custom application, the engineer should configure a parsing rule on the Broker VM. Parsing rules can be set to drop unnecessary data before it is ingested into Cortex XSIAM, preventing wasteful log volume and optimizing system efficiency.

Question 8

Question Type: MultipleChoice

A CISO has asked an engineer to create a custom dashboard in Cortex XSIAM that can be filtered to show incidents assigned to a specific user.

Which feature should be used to filter the incident data in the dashboard?

Options:

A- Filters and inputs in the custom dashboard
B- Report template to set the incident user filter
C- Visualization filter options in the widget configuration
D- Incident summary view to filter by user

Answer:

A

Explanation:

To show incidents assigned to a specific user in a Cortex XSIAM custom dashboard, the engineer should use filters and inputs in the custom dashboard. This enables dynamic filtering of incident data, allowing the dashboard to be customized based on user assignment.

Question 9

Question Type: MultipleChoice

A Behavioral Threat Protection (BTP) alert is triggered with an action of "Prevented (Blocked)" on one of several application servers running Windows Server 2022. The investigation determines the involved processes to be legitimate core OS binaries, and the description from the triggered BTP rule is an acceptable risk for the company to allow the same activity in the future.

This type of activity is only expected on the endpoints that are members of the endpoint group "AppServers," which already has a separate prevention policy rule with an exceptions profile named "Exceptions-AppServers" and a malware profile named "Malware-AppServers."

The CGO that was terminated has the following properties:

SHA256: eb71ea69dd19f728ab9240565e8c7efb59821e19e3788e289301e1e74940c208

File path: C:\Windows\System32\cmd.exe

Digital Signer: Microsoft Corporation

How should the exception be created so that it is scoped as narrowly as possible to minimize the security gap?

Options:

A- Create the exception via the alert itself, selecting the CGO hash, CGO signer, CGO process path, and applying the scope to the 'Exceptions-AppServers' profile.
B- Create a Disable Prevention Rule via Exceptions Configuration with the following selections:

C- Create a Legacy Agent Exception via Exceptions Configuration with the following selections:

D- Create the exception via the alert itself, selecting the CGO hash, CGO signer, CGO process path, and applying the scope to 'Global.'

Answer:

B

Explanation:

The most secure approach is to create a Disable Prevention Rule via Exceptions Configuration, scoped specifically to the Exceptions-AppServers profile. This rule should include the hash (SHA256), signer (Microsoft Corporation), and file path (C:\Windows\System32\cmd.exe). This ensures the exception is applied only to the trusted, legitimate process on the AppServers group while minimizing the security gap.

Question 10

Question Type: MultipleChoice

Which step must be taken to enable Cloud Identity Engine on Cortex XSIAM?

Options:

A- Enable SSO integration.
B- Activate it in the Customer Support Portal.
C- Activate it on HUB.
D- Enable Active Directory log collection.

Answer:

C

Explanation:

To enable Cloud Identity Engine on Cortex XSIAM, it must first be activated on HUB, Palo Alto Networks' centralized service management platform. Once activated, it can be configured and integrated with Cortex XSIAM for identity-based visibility and enforcement.